

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号
特開2000-165248
(P2000-165248A)

(43)公開日 平成12年6月16日(2000.6.16)

(51)Int.Cl. ⁷	識別記号	F I	テマコード*(参考)
H 0 3 M 7/00		H 0 3 M 7/00	5 C 0 6 3
G 0 9 C 5/00		G 0 9 C 5/00	5 C 0 7 6
H 0 4 N 1/387		H 0 4 N 1/387	5 J 0 6 4
7/08		7/08	Z 5 J 1 0 4
7/081			9 A 0 0 1
審査請求 未請求 請求項の数36 O L (全 15 頁)			

(21)出願番号 特願平10-337258

(22)出願日 平成10年11月27日(1998.11.27)

(71)出願人 000001007

キヤノン株式会社

東京都大田区下丸子3丁目30番2号

(72)発明者 吉田 淳

東京都大田区下丸子3丁目30番2号 キヤ
ノン株式会社内

(72)発明者 岩村 恵市

東京都大田区下丸子3丁目30番2号 キヤ
ノン株式会社内

(74)代理人 100090273

弁理士 國分 孝悦

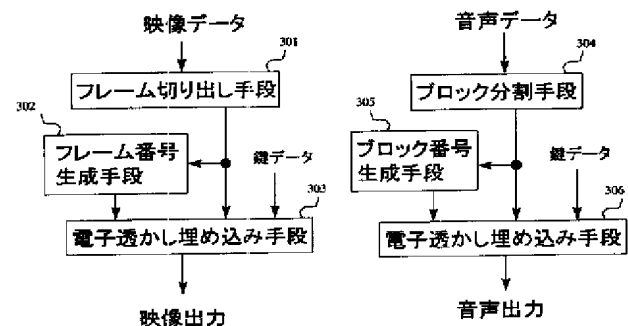
最終頁に続く

(54)【発明の名称】 電子透かし埋め込み装置、出力制御装置及びコンピュータ読み取り可能な記憶媒体

(57)【要約】

【課題】 映像と音声を含むコンテンツの著作権を、映像と音声に対して総合的に保護できる電子透かしを上記コンテンツに埋め込む。

【解決手段】 入力された映像データはフレーム切り出し手段301によりフレーム分割され、各フレームにフレーム番号が付加される。そして、各フレームとフレーム番号と不揮発性メモリ107に記憶されている電子透かし埋め込み位置情報等の鍵データとが電子透かし埋め込み手段303に入力され、各フレームにフレーム番号が電子透かしとして埋め込まれる。音声データもブロック分割手段304でブロックに分割され、ブロック番号が付加され、各ブロックとブロック番号と鍵データとが電子透かし埋め込み手段306に入力され、各ブロックにブロック番号が電子透かしとして埋め込まれる。



【特許請求の範囲】

【請求項1】 複数の情報系列を含むコンテンツにおける上記各情報系列に対してそれぞれ埋め込み情報を生成する情報生成手段と、
上記生成された各埋め込み情報を各情報系列に対して電子透かしとして埋め込む埋め込み手段とを設けたことを特徴とする電子透かし埋め込み装置。

【請求項2】 上記情報生成手段が生成する各埋め込み情報が、互いに関連する情報であることを特徴とする請求項1記載の電子透かし埋め込み装置。

【請求項3】 上記情報生成手段が生成する各埋め込み情報が、一致することを特徴とする請求項1記載の電子透かし埋め込み装置。

【請求項4】 上記情報系列を分割して部分情報系列を生成する分割手段を設けると共に、上記情報生成手段は、上記部分情報系列を識別する識別子を生成し、上記埋め込み手段は、上記部分情報系列に上記生成された識別子を電子透かしとして埋め込むことを特徴とする請求項1記載の電子透かし埋め込み装置。

【請求項5】 上記識別子が番号であることを特徴とする請求項4記載の電子透かし埋め込み装置。

【請求項6】 上記各情報系列に埋め込まれる上記埋め込み情報を組み合わせることにより一つの情報を表すことを特徴とする請求項1記載の電子透かし埋め込み装置。

【請求項7】 上記埋め込み情報の少なくとも1つが誤り訂正符号化されていることを特徴とする請求項1記載の電子透かし埋め込み装置。

【請求項8】 上記埋め込み情報を組み合わせることによって表される情報が誤り訂正符号化されていることを特徴とする請求項6記載の電子透かし埋め込み装置。

【請求項9】 上記情報生成手段が、上記情報系列のうちの少なくとも一つから演算によって埋め込み情報を生成し、上記埋め込み手段が、上記埋め込み情報を、上記情報系列のうちの少なくとも他の一つに電子透かしとして埋め込むことを特徴とする請求項1記載の電子透かし埋め込み装置。

【請求項10】 上記情報生成手段が、上記埋め込み情報として、上記情報系列の全体又は所定の部分の圧縮値を求めることを特徴とする請求項9記載の電子透かし埋め込み装置。

【請求項11】 上記情報生成手段によって生成された上記埋め込み情報を暗号化する暗号化手段を設けたことを特徴とする請求項9記載の電子透かし埋め込み装置。

【請求項12】 上記情報生成手段が、上記埋め込み方法として、上記情報系列の全体又は所定の部分のデジタル署名を求めることを特徴とする請求項9記載の電子透かし埋め込み装置。

【請求項13】 上記情報系列のうち少なくとも二つを分割して部分情報系列を生成する分割手段を設け、上記

情報生成手段は、上記情報系列のうちの少なくとも一つより生成された上記部分情報系列を埋め込み情報とし、上記埋め込み手段は、上記埋め込み情報を、上記情報系列のうちの少なくとも他の一つより生成された部分情報系列に電子透かしとして埋め込むことを特徴とする請求項1記載の電子透かし埋め込み装置。

【請求項14】 上記埋め込み情報である上記部分情報系列を暗号化する暗号化手段を設けたことを特徴とする請求項13記載の電子透かし埋め込み装置。

10 【請求項15】 上記情報系列のうち少なくとも一つを暗号化する暗号化手段を設けると共に、上記情報生成手段は、上記暗号化を復号するための復号鍵を埋め込み情報として生成し、上記埋め込み手段が、上記復号鍵の埋め込み情報を情報系列の少なくとも他の一つに埋め込むことを特徴とする請求項1記載の電子透かし埋め込み装置。

【請求項16】 上記複数の情報系列が音声情報及び映像情報であることを特徴とする請求項1記載の電子透かし埋め込み装置。

20 【請求項17】 上記複数の情報系列が複数のオブジェクトを表すデータを含むコンテンツ中の所定のオブジェクトを表すデータであることを特徴とする請求項1記載の電子透かし埋め込み装置。

【請求項18】 複数の情報系列を含むコンテンツを出力する出力手段と、
上記コンテンツにおける上記各情報系列を分割して部分情報系列とする分割手段と、

上記各部分情報系列に電子透かしとして埋め込まれている埋め込み情報を抽出する電子透かし抽出手段と、

30 上記抽出された各埋め込み情報を比較し、比較結果に応じて上記出力手段を制御する比較手段とを設けたことを特徴とする出力制御装置。

【請求項19】 複数の情報系列を含むコンテンツを出力する出力手段と、

上記コンテンツにおける上記各情報系列を分割して部分情報系列とする分割手段と、

上記各部分情報系列に電子透かしとして埋め込まれている埋め込み情報を抽出する電子透かし抽出手段と、

上記埋め込み情報の一つに対して演算を行う演算手段

40 と、

上記演算手段により求められた値と上記部分情報系列とを比較し、比較結果に応じて上記出力手段を制御する比較手段とを設けたことを特徴とする出力制御装置。

【請求項20】 上記演算手段は、上記部分情報系列の全体又は一部分の圧縮値を求めることを特徴とする請求項19記載の出力制御装置。

【請求項21】 上記電子透かし抽出手段が抽出した上記埋め込み情報に施されている暗号化を復号する復号手段を設けたことを特徴とする請求項19記載の出力制御装置。

【請求項22】 上記演算手段によって求められた演算結果を暗号化する暗号化手段を設けたことを特徴とする請求項19記載の出力制御装置。

【請求項23】 上記コンテンツに含まれる複数の情報系列が、映像情報及び音声情報であることを特徴とする請求項18又は19記載の出力制御装置。

【請求項24】 上記コンテンツに含まれる情報系列が、複数のオブジェクトを表すデータを含むコンテンツ中の所定のオブジェクトを表すデータであることを特徴とする請求項18又は19記載の出力制御装置。

【請求項25】 複数の情報系列を含むコンテンツにおける上記各情報系列の少なくとも一つの情報系列を分割して部分情報系列とする分割手段と、
上記部分情報系列に電子透かしとして埋め込まれている埋め込み情報を抽出する電子透かし抽出手段と、
上記埋め込み情報を上記コンテンツに含まれる情報系列の一つとして出力する出力手段を設けたことを特徴とする出力制御装置。

【請求項26】 上記電子透かし抽出手段により抽出された埋め込み情報に施されている暗号の復号を行う復号手段を設けたことを特徴とする請求項25記載の出力制御装置。

【請求項27】 上記コンテンツに含まれる複数の情報系列が映像情報及び音声情報であると共に、上記電子透かしが埋め込まれる被埋め込み情報が音声又は映像情報であり、上記埋め込み情報が映像又は音声情報であることを特徴とする請求項25記載の出力制御装置。

【請求項28】 上記コンテンツに含まれる情報系列、上記被埋め込み情報及び上記埋め込み情報が、複数のオブジェクトを表すデータを含むコンテンツ中の所定のオブジェクトを表すデータであることを特徴とする請求項25記載の出力制御装置。

【請求項29】 少なくとも一つの暗号化された情報系列と少なくとも一つの電子透かしが埋め込まれた情報系列とを含む複数の情報系列を含むコンテンツにおける上記電子透かしが埋め込まれた情報系列から埋め込み情報を抽出する抽出手段と、
上記埋め込み情報を復号鍵として上記情報系列に施された暗号を復号する復号手段を設けたことを特徴とする出力制御装置。

【請求項30】 上記暗号化された情報系列が映像又は音声情報であり、上記電子透かしが埋め込まれた情報系列が音声又は映像情報であることを特徴とする請求項29記載の出力制御装置。

【請求項31】 上記暗号化された情報系列及び上記電子透かしが埋め込まれた情報系列が、複数のオブジェクトを表すデータを含むコンテンツ中の所定のオブジェクトを表すデータであることを特徴とする請求項29記載の出力制御装置。

【請求項32】 複数の情報系列を含むコンテンツにお

ける上記各情報系列に対してそれぞれ埋め込み情報を生成する処理と、

上記生成された各埋め込み情報を各情報系列に対して電子透かしとして埋め込む処理とを実行するためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項33】 複数の情報系列を含むコンテンツを出力する処理と、

上記コンテンツにおける上記各情報系列を分割して部分情報系列とする処理と、

10 上記各部分情報系列に電子透かしとして埋め込まれている埋め込み情報を抽出する処理と、

上記抽出された各埋め込み情報を比較し、比較結果に応じて上記出力を制御する処理とを実行するためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項34】 複数の情報系列を含むコンテンツを出力する処理と、

上記コンテンツにおける上記各情報系列を分割して部分情報系列とする処理と、

20 上記各部分情報系列に電子透かしとして埋め込まれている埋め込み情報を抽出する処理と、

上記埋め込み情報の一つに対して演算を行う処理と、
上記演算により求められた値と上記部分情報系列とを比較し、比較結果に応じて上記出力を制御する処理とを実行するためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項35】 複数の情報系列を含むコンテンツにおける上記各情報系列の少なくとも一つの情報系列を分割して部分情報系列とする処理と、

30 上記部分情報系列に電子透かしとして埋め込まれている埋め込み情報を抽出する処理と、

上記埋め込み情報を上記コンテンツに含まれる情報系列の一つとして出力する処理とを実行するためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項36】 少なくとも一つの暗号化された情報系列と少なくとも一つの電子透かしが埋め込まれた情報系列とを含む複数の情報系列を含むコンテンツにおける上記電子透かしが埋め込まれた情報系列から埋め込み情報を抽出する抽出処理と、

40 上記埋め込み情報を復号鍵として上記情報系列に施された暗号を復号する処理とを実行するためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ビデオ、テレビ番組、映画等の映像及び音声を含むコンテンツに対して著作権保護のための電子透かしを埋め込む場合に用いて好適な電子透かし埋め込み装置、及び記録された上記コンテンツの再生出力等の出力制御に用いて好適な出力制御装置、及びそれらに用いられるコンピュータ読み取り可能な記憶媒体に関するものである。

【0002】

【従来の技術】従来より、画像、音楽、映画等のコンテンツの不正なコピーを防ぐための手法の一つとして電子透かしと呼ばれる手法がある。電子透かしとは、不正を防止するための情報を、人間に知覚できない形でコンテンツに埋め込む手法である。その場合、デジタルコンテンツはそのままの状態では情報を埋め込むが、アナログコンテンツはデジタル化した後、情報を埋め込む。

【0003】以下、コンテンツに対する電子透かしの従来の埋め込み方法の代表的なものについて述べる。静止画像に対する電子透かしの情報埋め込み方式の代表的なものとして、デジタル画像の場合でいえば、画素の色相、明度等にあたる、デジタルコンテンツのデータ値に演算を施して電子透かしを埋め込む手法がある。この手法の代表的なものとして、デジタルコンテンツをブロックに分割し、ブロック毎に+1と-1の組み合わせである予め決められた透かしパターンを足し込むというDigimar社、米国特許5,636,292号の手法がある。

【0004】他の静止画像に対する電子透かし埋め込み方法として、デジタルコンテンツに対して、高速フーリエ変換、離散コサイン変換、ウェーブレット変換等の周波数変換を行い、周波数領域に透かし情報を加えた後、逆周波数変換を行うことにより埋め込みを行う手法がある。

【0005】上記高速フーリエ変換による手法では、入力コンテンツは、PN系列を加えられて拡散された後、ブロックに分割される。そして、ブロック毎にフーリエ変換が施され、1ブロックに1ビットの透かし情報が埋め込まれる。この透かし情報が埋め込まれたブロックは逆フーリエ変換が施され、再び最初と同じPN系列が加えられて電子透かしが埋め込まれたコンテンツが得られる。これは、大西、岡、松井、"PN系列による画像への透かし署名法"1997年、暗号と情報セキュリティシンポジウム講演論文集、SCIS97-26Bに詳しい。

【0006】離散コサイン変換による手法は、ブロックに分割し、ブロック毎に離散コサイン変換をする。そして、1ブロックに1ビットの情報を埋め込んだ後、逆変換をして電子透かし埋め込み済みコンテンツを生成する。これは、中村、小川、高嶋、"デジタル画像の著作権保護のための周波数領域における電子透かし方式"1997年、暗号と情報セキュリティシンポジウム講演論文集、SCIS97-26Aに詳しい。

【0007】ウェーブレット変換による手法は、入力コンテンツをブロック分割する必要のない手法である。これは、石塚、酒井、櫻井、"ウェーブレット変換を用いた電子透かし技術の安全性と信頼性に関する実験的考察"1997年、暗号と情報セキュリティシンポジウム講演論文集、SCIS97-26Dに詳しい。

【0008】音声データの場合も、静止画像と同様に、ブロック化した後に周波数変換、電子透かしの埋め込み、逆周波数変換を行う方法により、電子透かしの埋め込みが可能である。具体的には、周期の異なる三角関数を基底関数群として、それらの1次結合の形で表される1次元音声データの基底関数群から幾つかの基底関数を取り出し、位相をいくらかずらした後、再び音声データに復元しても、元のデータとの違いを知覚することができないという人間の聴覚特性を利用した方法がある。

【0009】また、1次元実数値関数として表されるデジタル音声データをウェーブレット変換して、得られたウェーブレット係数に対し埋め込みを行うという方法がある。この方法は、静かな音は、大きな音にかき消されてしまうという聴覚特性を利用したものである。これらの手法の詳細については、井上杉「電子透かし—マルチメディア自体の暗号システム」丸山学芸図書に詳しい。

【0010】また、電子透かしの静止画像への埋め込み、音声への埋め込みの他、動画像データへの電子透かし埋め込み技術として、動きベクトルに埋め込む方法や、2台の微妙に異なる角度から被写体を撮影するカメラからの動画像を組み合わせる方法が知られている。

【0011】次に、一般的なフレーム内符号化手段とフレーム間符号化手段を備えた動画像圧縮方式MPEGの原理について説明した後、電子透かしを動画像データの動きベクトルに埋め込む手法について説明する。MPEGでは、フレーム間の差分を取ることで時間軸方向の冗長度を落とし、これによって得られた差分データをDCT及び可変長符号化処理して空間方向の冗長度を落とすことによって全体として高能率符号化を実現する。上記時間軸方向の冗長度については、動画の場合には連続したフレームの相関が高いことに着目し、符号化しようとするフレームと時間的に先行又は後行するフレームとの差分をとることによって冗長度を落とすことが可能となる。

【0012】そこで、フレーム内で符号化する符合化モードで得られるインドラ符号化画像(I-ピクチャ)の他に、時間的に先行するフレームとの差分値を符号化する前方予測符号化画像(P-ピクチャ)と、時間的に先行するフレーム又は後行するフレームとの差分値、或いはそれらの両フレームからの補間フレームとの差分値の内最もデータ量が少ないものを符号化する両方向予測符号化画像(B-ピクチャ)とを有し、これらの符合化モードによる各フレームを所定の順序で組み合わせている。

【0013】MPEGにおいては、上述のI-ピクチャ、P-ピクチャ、B-ピクチャをそれぞれ1枚、4枚、10枚で1単位(GOP)とし、先頭にI-ピクチャを配し、2枚のB-ピクチャとP-ピクチャとを繰り返して配する組み合わせを推奨しており、一定周期でI-

ピクチャを置くことによって、逆再生等の特殊再生やこのGOPを単位とした部分再生を可能とするとともにエラー伝播の防止を図っている。

【0014】また、フレーム中で新たな物体が現れた場合には、時間的に先行するフレームとの差分を取るよりも、後行するフレームとの差分を取った方がその差分値が少なくなる場合がある。そこで、MPEGでは、上述のような両方向予測符号化を行い、より高効率な圧縮を行っている。

【0015】また、MPEGでは動き補償を行う。即ち、8画素×8画素のブロックを輝度データについて4ブロック、色差データについて2ブロック集めた所定ブロック（マクロブロック）単位で、先行又は後行フレームの対応ブロック近傍のマクロブロックとの差分をとり、一番差が少ないマクロブロックを探索することによって動きベクトルを検出し、この動きベクトルをデータとして符号化する。

【0016】復号の際には、この動きベクトルを用いて先行又は後行フレームの対応マクロブロックデータを抽出し、これによって動き補償を用いて符号化された符号化データの復号を行う。上述のような動き補償に際しては、時間的に先行するフレームを一旦符号化した後、再度復号したフレームを得て先行フレームとし、このフレームにおけるマクロブロックと符号化しようとするフレームのマクロブロックとを用いて動き補償が行われる。

【0017】そこで、電子透かしを動きベクトルに埋め込む方式では、一つの動きベクトルの移動を透かし情報のビット列の1ビットに対応させる。即ち、このビットの値を1にしたい場合は、このベクトルを目視では認識不可能な程度移動させ、値を0にしたい場合には、ベクトルを移動させない。この処理を多くの動きベクトルに施すことにより、全ての透かし情報を埋め込む方法を取っている。

【0018】また、現在標準化作業中のMPEG-4においては、複数ビデオプレーンを重ね合わせる処理が導入された。これによりマクロブロックごとの符号化に代わり、画像上のオブジェクト単位での符号化など、任意の輪郭の領域での処理が可能となった。輪郭符号化にはMMRや算術符号化が使われる。

【0019】次に、2台の微妙に異なる角度より被写体を撮影するカメラからの動画を組み合わせる方法について説明する。一つの被写体に対して微妙に異なる角度から撮影できるように2台のカメラを設置する。被写体を頂点として2台のカメラがなす角度は、非常に小さいので、2台のカメラで撮影した画像は、人間の目では識別できない。

【0020】2台のカメラをA、Bとする。カメラA、Bにより撮影した画像を各々フレーム毎に分割し、それらを(a1, a2, ..., an)、(b1, b2, ..., bn)とする。カメラA、Bが撮影した画像のフレー

ムよりランダムに画像を選択し、原画像を作成する。例えば、原画像は(a1, a2, b3, a4, b5, ..., bn)となる。ここで、1フレームを透かし情報のビット列の1ビットに対応させる。即ち、このビットの値を1にしたい場合は、フレームを他方のフレームで置き換える。ビットの値を0にしたい場合は、フレームの置き換えを行わない。この処理を多くのフレームに施すことにより、全ての透かし情報を埋め込む。

【0021】

10 【発明が解決しようとする課題】従来の、映画等の映像と音声とを有するコンテンツに対する電子透かし埋め込み方式は、映像及び音声に対してそれぞれ別個に埋め込みを行うものであった。このため、映像、音声各々単体での著作権は保護することが可能であったが、映像と音声の両方を有するコンテンツとして総合的に著作権を保護するには限界があった。

20 【0022】本発明は、上記の問題を解決するために成されたもので、映像及び音声のコンテンツの著作権を総合的に保護できる電子透かしを埋め込むことができるようにすることを目的としている。

【0023】

【課題を解決するための手段】上記の目的を達成するために、本発明による電子透かし埋め込み装置においては、複数の情報系列を含むコンテンツにおける上記各情報系列に対してそれぞれ埋め込み情報を生成する情報生成手段と、上記生成された各埋め込み情報を各情報系列に対して電子透かしとして埋め込む埋め込み手段とを設けている。

30 【0024】また、本発明による出力制御装置においては、複数の情報系列を含むコンテンツを出力する出力手段と、上記コンテンツにおける上記各情報系列を分割して部分情報系列とする分割手段と、上記各部分情報系列に電子透かしとして埋め込まれている埋め込み情報を抽出する電子透かし抽出手段と、上記抽出された各埋め込み情報を比較し、比較結果に応じて上記出力手段を制御する比較手段とを設けている。

【0025】また、本発明による他の出力制御装置においては、複数の情報系列を含むコンテンツを出力する出力手段と、上記コンテンツにおける上記各情報系列を分割して部分情報系列とする分割手段と、上記各部分情報系列に電子透かしとして埋め込まれている埋め込み情報を抽出する電子透かし抽出手段と、上記埋め込み情報の一つに対して演算を行う演算手段と、上記演算手段により求められた値と上記部分情報系列とを比較し、比較結果に応じて上記出力手段を制御する比較手段とを設けている。

50 【0026】また、本発明による他の出力制御装置においては、複数の情報系列を含むコンテンツにおける上記各情報系列の少なくとも一つの情報系列を分割して部分情報系列とする分割手段と、上記部分情報系列に電子透

かしとして埋め込まれている埋め込み情報を抽出する電子透かし抽出手段と、上記埋め込み情報を上記コンテンツに含まれる情報系列の一つとして出力する出力手段を設けている。

【0027】また、本発明による他の出力制御装置においては、少なくとも一つの暗号化された情報系列と少なくとも一つの電子透かしが埋め込まれた情報系列とを含む複数の情報系列を含むコンテンツにおける上記電子透かしが埋め込まれた情報系列から埋め込み情報を抽出する抽出手段と、上記埋め込み情報を復号鍵として上記情報系列に施された暗号を復号する復号手段を設けている。

【0028】また、本発明による記憶媒体においては、複数の情報系列を含むコンテンツにおける上記各情報系列に対してそれぞれ埋め込み情報を生成する処理と、上記生成された各埋め込み情報を各情報系列に対して電子透かしとして埋め込む処理とを実行するためのプログラムを記憶している。

【0029】また、本発明による他の記憶媒体においては、複数の情報系列を含むコンテンツを出力する処理と、上記コンテンツにおける上記各情報系列を分割して部分情報系列とする処理と、上記各部分情報系列に電子透かしとして埋め込まれている埋め込み情報を抽出する処理と、上記抽出された各埋め込み情報を比較し、比較結果に応じて上記出力を制御する処理とを実行するためのプログラムを記憶している。

【0030】また、本発明による他の記憶媒体においては、複数の情報系列を含むコンテンツを出力する処理と、上記コンテンツにおける上記各情報系列を分割して部分情報系列とする処理と、上記各部分情報系列に電子透かしとして埋め込まれている埋め込み情報を抽出する処理と、上記埋め込み情報の一つに対して演算を行う処理と、上記演算により求められた値と上記部分情報系列とを比較し、比較結果に応じて上記出力を制御する処理とを実行するためのプログラムを記憶している。

【0031】また、本発明による他の記憶媒体においては、複数の情報系列を含むコンテンツにおける上記各情報系列の少なくとも一つの情報系列を分割して部分情報系列とする処理と、上記部分情報系列に電子透かしとして埋め込まれている埋め込み情報を抽出する処理と、上記埋め込み情報を上記コンテンツに含まれる情報系列の一つとして出力する処理とを実行するためのプログラムを記憶している。

【0032】また、本発明による他の記憶媒体においては、少なくとも一つの暗号化された情報系列と少なくとも一つの電子透かしが埋め込まれた情報系列とを含む複数の情報系列を含むコンテンツにおける上記電子透かしが埋め込まれた情報系列から埋め込み情報を抽出する抽出処理と、上記埋め込み情報を復号鍵として上記情報系列に施された暗号を復号する処理とを実行するためのプロ

グラムを記憶している。

【0033】

【発明の実施の形態】以下、本発明の実施の形態を図面と共に説明する。図1は、本発明による電子透かし埋め込み装置の実施の形態を示すブロック図である。本装置は、例えば、再生側と録画側の2台のビデオテープレコーダに接続されて用いられる。再生側ビデオテープレコーダでは、電子透かしを埋め込む前のオリジナルのビデオテープを再生する。再生された映像及び音声は、それぞれ映像出力端子及び音声出力端子から電子透かし埋め込み装置に入力される。また、電子透かし埋め込み装置によって電子透かしが埋め込まれた映像及び音声は、録画側ビデオテープレコーダに入力されて記録される。

【0034】本装置は、アナログの映像信号を本装置へ取り込む映像入力装置101、アナログの音声信号を本装置へ取り込む音声入力装置102、入力された映像又は音声をデジタルデータに変換するA/D変換装置103、104、電子透かし埋め込み装置105を有する。

【0035】上記電子透かし埋め込み装置105は、外部からの入力を受ける、又は本装置に入力された映像又は音声データから演算によって、情報を生成する等の方法によって、電子透かしとして埋め込む埋め込み情報を生成し、さらに、不揮発性メモリ107に保存されている電子透かしを埋め込む位置を示す座標情報等の鍵データを用い、生成した埋め込み情報を電子透かしとしてコンテンツに埋め込むものである。

【0036】本装置はさらに、一時的にデータを保存するために用いられる揮発性メモリ106、電子透かし埋め込みの埋め込み位置を示す座標データ等から成る鍵データ等が保存される不揮発性メモリ107、本装置に搭載されている各装置を制御し、本実施の形態による電子透かし埋め込み方式を実行するコントローラ108、本装置で電子透かしの埋め込み処理が行われたデジタルデータをアナログデータに変換するD/A変換装置109、110、本装置によって電子透かしを埋め込まれた映像及び音声を、ビデオテープレコーダ等に対して出力する映像出力装置111及び音声出力装置112、本装置を構成する各装置間でデジタルデータを交換するのに用いられるデータバス113を有している。

【0037】次に動作について説明する。再生側ビデオテープレコーダで再生され、その映像出力端子から出力されたアナログ画像データは、本電子透かし埋め込み装置の映像入力装置101から入力され、A/D変換装置103でデジタルデータに変換されて、揮発性メモリ106に保存される。同様に再生側ビデオテープレコーダの音声出力端子から出力されたアナログ音声データは、音声入力装置102から入力され、A/D変換装置104によりデジタルデータに変換されて、揮発性メモリ106に保存される。

【0038】電子透かし埋め込み装置105では、揮発性メモリ106に保存されている映像及び／又は音声データを用いて演算を行う、或いは外部から入力を受ける等の方法で、電子透かしとして埋め込む埋め込みデータを生成する。次に、電子透かし埋め込み装置105は、不揮発性メモリ107に保存されている鍵データを用いて、上記生成した埋め込みデータを電子透かしとして映像及び／又は音声データに埋め込む。

【0039】電子透かしが埋め込まれた映像及び／又は音声データは各々D/A変換装置109、110によりアナログ化される。アナログ化された映像信号は、映像出力装置111により録画側ビデオテーブルコードの映像入力端子に入力され、アナログ化された音声信号は、音声出力装置112により録画側ビデオテーブルコードの音声入力端子に入力されて、それぞれ記録される。

【0040】図2は、図1の電子透かし埋め込み装置により電子透かしが埋め込まれたコンテンツに対して、不正に字幕を入れる、吹き替えを行う等の改竄処理が施された場合に、コンテンツが記録されている記録媒体を再生できないようにした本発明による出力装置の実施の形態を示す。

【0041】本出力装置は、記録媒体に記憶されている信号を読み取り、音声信号と映像信号に分離して出力するデッキ部201、出力制御装置207により制御される音声出力装置202、同様に出力制御装置207により制御される映像出力装置203、デッキ部201が出力した音声信号及び映像信号をディジタル化して音声データ及び映像データに変換するA/D変換装置204、205、装置を構成する各装置を制御し、本実施の形態による出力方式を実行するコントローラ206を有している。

【0042】さらに、出力制御装置207、一時的にデータや、演算の途中結果などを保存するために用いられる揮発性メモリ208、電子透かし埋め込みのための埋め込み位置を示す座標情報等から成る鍵データ等が保存される不揮発性メモリ209、本装置を構成する各装置間でディジタルデータを交換するのに用いられるデータバス210を有している。

【0043】次に動作について説明する。デッキ部201において記録媒体が再生されると、記録媒体に記録されている信号が読み取られ、音声信号と映像信号に分離される。音声信号は音声出力装置202に、映像信号は映像出力装置203にそれぞれ入力され一時的に保存される。また、音声信号はA/D変換装置204、映像信号はA/D変換装置205によりそれぞれディジタルデータ（音声データ及び映像データ）に変換され、揮発性メモリ208に一時的に保存される。

【0044】出力制御装置207は、揮発性メモリ208より音声データと映像データを取得し、不揮発性メモリ209に保存されている鍵データ等を用い、電子透かし

しとして映像データ、及び／又は音声データに埋め込まれている情報を抽出し、その結果により、音声出力装置202、映像出力装置203による音声出力、映像出力を決定又は制御する。

【0045】次に、電子透かし埋め込み装置105による具体的な埋め込みデータの生成と電子透かしの埋め込み処理、及び出力制御装置207による出力制御処理の各実施の形態について説明する。

【0046】図3は、電子透かし埋め込み装置105で行われる電子透かし埋め込み方式の第1の実施の形態を示すブロック図である。本方式においては、映像をフレームに分割し、各々のフレームにフレーム番号を割り当て、割り当てたフレーム番号を電子透かしとして各フレームに埋め込む。また、音声をブロックに分割し、各々のブロックにブロック番号を割り当て、割り当てたブロック番号を電子透かしとして各ブロックに埋め込む。

【0047】本方式は、映像データをフレーム毎に分割するフレーム切り出し手段301、フレームに先頭から順に番号を付けるフレーム番号生成手段302、映像の各フレームにフレーム番号を埋め込む電子透かし埋め込み手段303、音声データをブロックに分割するブロック分割手段304、音声ブロックに先頭から順に番号を付けるブロック番号生成手段305、音声の各ブロックにブロック番号を埋め込む電子透かし埋め込み手段306から構成される。

【0048】次に動作について説明する。入力された映像データはフレーム切り出し手段301により、フレームに分割され、順に出力される。出力された各フレームはフレーム番号生成手段302に入力され、順にフレーム番号が生成される。また、各フレームとフレーム番号生成手段302により生成されたフレーム番号と不揮発性メモリ107に記憶されている電子透かしを埋め込む位置を示す座標情報等からなる鍵データとが電子透かし埋め込み手段303に入力され、フレーム番号が各フレームに電子透かしとして埋め込まれ出力される。尚、鍵データが不揮発性メモリから読み込まれず、外部記憶装置等から入力される場合等の場合もある。

【0049】音声データについても同様に、ブロック分割手段304により、分割されたブロックがブロック番号生成手段305に入力され、ブロック番号が生成される。また、各ブロックとブロック番号生成手段305によって生成されたブロック番号と電子透かしを埋め込む位置を示す座標情報等からなる鍵データとが電子透かし埋め込み手段306に入力され、ブロック番号が各ブロックに電子透かしによって埋め込まれ出力される。

【0050】ここでの映像出力、音声出力は揮発性メモリ106に一時的に保存され同期を取られた後に、D/A変換装置109、110によりアナログデータに変換され、映像出力装置111、音声出力装置112から出力される。

【0051】図4は、図3の電子透かし埋め込み方式に対応する出力制御方式の第1の実施の形態を示すブロック図であり、図2における出力制御装置207に用いられるものである。図4の方式は、図3のフレーム切り出し手段と同じ動作を行うフレーム切り出し手段401、映像の各フレームから電子透かしとして埋め込まれているフレーム番号を抽出する電子透かし抽出手段402、図3のブロック分割手段と同じ動作を行うブロック分割手段403、音声の各ブロックから電子透かしとして埋め込まれているブロック番号を抽出する電子透かし抽出手段404、ブロック番号とフレーム番号とを比較し、正しい対応をしているかを調べる比較手段405から構成される。

【0052】次に動作について説明する。入力された映像データはフレーム切り出し手段401に入力され、フレーム毎に分割される。各フレームは、電子透かしが埋め込んである位置を示す座標情報等からなる鍵データと共に電子透かし埋め込み手段402に入力され、フレーム番号が抽出される。また、入力された音声データは、ブロック分割手段403に入力されてブロックに分割され、電子透かし抽出手段404において鍵データにより各ブロックからブロック番号が抽出される。

【0053】電子透かし抽出手段402により抽出されたフレーム番号と電子透かし抽出手段404により抽出されたブロック番号は比較手段405に入力され、正しい対応をしていた場合は、通常出力を許可する信号を発し、この信号により、音声は音声出力装置202から、映像は映像出力装置203からそれぞれ出力される。

【0054】図5は、電子透かし埋め込み方式の第2の実施の形態を示すブロック図である。本方式は映像データ、音声データの他に情報の入力を受け、映像と音声に入力された情報を符号化して埋め込むものである。

【0055】本方式は、映像データをフレーム毎に分割するフレーム切り出し手段501、音声データをブロックに分割するブロック分割手段502、外部より埋め込み情報を入力する情報入力手段503、入力されたデータを埋め込み情報とする符号化手段504、映像のフレームに埋め込み情報を電子透かしとして埋め込む電子透かし埋め込み手段505、音声のブロックに埋め込み情報を電子透かしとして埋め込む電子透かし埋め込み手段506から構成される。

【0056】入力された映像データはフレーム切り出し手段501によって、また音声データはブロック分割手段502によって各々フレーム、ブロックに分割される。またキーボード等の情報入力手段503によって入力された電子透かしとして埋め込まれる埋め込み情報は、符号化手段504によって、誤り訂正符号化等の符号化が施される。符号化された埋め込み情報は、フレーム、鍵データと共に電子透かし埋め込み手段505に入力され、電子透かしとして映像のフレームに埋め込まれ

る。

【0057】また、埋め込み情報はブロック、鍵データと共に電子透かし埋め込み手段506に入力され、電子透かしとして音声のフレームに埋め込まれる。この時、電子透かしは全ての映像フレーム、音声ブロックに埋め込まれる場合の他、一部の映像フレーム、音声ブロックに埋め込まれる場合がある。

【0058】また、図4の出力制御方式において、比較手段405で、所定の映像フレームに埋め込まれている情報と、所定の音声ブロックに埋め込まれている情報とを比較することにより、図5の電子透かし埋め込み方式に対応する出力制御方式を構成できる。この際、埋め込み情報が誤り訂正符号化されている場合は、比較手段405は、情報の比較を行う前に誤り訂正符号の復号を行う。

【0059】図5において、符号化手段504が埋め込み情報の誤り訂正符号化を行い、情報ビット又は冗長ビットの一方を映像フレームに、他方を音声ブロックに書き込む電子透かし埋め込み方式も容易に実現可能である。また、図4において、比較手段405で、情報ビットを誤り訂正符号化し、求めた冗長ビットと、電子透かしから抽出した冗長ビットとを比較することにより、対応する出力制御方式も容易に構成できる。

【0060】図5において、符号化手段504が所定の埋め込み情報を二つのビット列に分解し、一方を映像フレームに、他方を音声ブロックに埋め込む電子透かし埋め込み方式も容易に実現可能である。また、図4の出力制御方式において、比較手段405で、抽出された2つの情報を合成し復元した埋め込み方法が上記所定の情報と一致していることを確認することにより、対応する出力制御方式も容易に構成できる。

【0061】図6は、電子透かし埋め込み方式の第3の実施の形態を示すブロック図である。本方式は、映像フレーム数と同じ数のブロックに音声データを分割し、映像フレームと音声ブロックとを一对一に対応させ、映像フレームに対応する音声ブロックを埋め込むものである。

【0062】本方式は、映像データをフレームに分割し、1フレームずつ出力するフレーム切り出し手段601、映像フレームの1フレームの表示時間と同じ長さに音声データを分割しブロックとするブロック分割手段602、映像フレームに音声ブロックを埋め込む電子透かし埋め込み手段603から構成される。

【0063】入力された映像データは、フレーム分割手段601によって、フレーム毎に分割され、順に出力される。また、入力された音声データは、ブロック分割手段602によって、映像フレームと同じ数に分割され、順に出力される。フレーム分割手段601とブロック分割手段602の出力を受ける電子透かし埋め込み手段603では、電子透かしを埋め込む位置を示す座標情報等

からなる鍵データにより、フレームに、音声ブロックが電子透かしとして埋め込まれて出力される。

【0064】図7は、図6の電子透かし埋め込み方式に対応する出力制御方式の第2の実施の形態を示すブロック図である。本方式は、映像をフレームに分割するフレーム切り出し手段701、映像フレームに埋め込まれている音声ブロックを抽出する電子透かし抽出手段702、D/A変換手段703からなる。D/A変換手段703は、一例として音声出力装置202によって処理が実行されるものとする。

【0065】デッキ部201で媒体より読み込まれた映像信号は映像出力装置203に入力されるのと同時に、A/D変換装置205によりデジタルデータに変換される。デジタルデータに変換された映像データは、フレーム切り出し手段701によってフレーム毎に分割され、電子透かし抽出手段702において、鍵データより、埋め込まれている音声ブロックが抽出される。抽出された音声ブロックは、D/A変換手段703によりアナログデータ化され、音声出力装置202によって出力される。

【0066】図8は電子透かし埋め込み方式の第4の実施の形態を示すブロック図である。本方式では、音声データを映像フレーム数と同じ数のブロックに分割し、映像フレームと音声ブロックとを一对一に対応させる。また、各々の音声ブロックを暗号化し、暗号化音声ブロックを対応する映像フレームに埋め込む。

【0067】本方式は、図6と同様の動作を行うフレーム切り出し手段601、ブロック分割手段602、電子透かし埋め込み手段603、及び暗号化手段801から構成される。ここで用いられる暗号化には、DES等の共通鍵暗号化方式、RSA等の公開鍵暗号化方式が用いられる（各暗号の詳細は岡本栄司著「暗号理論入門」共立出版株式会社参照）。

【0068】入力された音声データは、ブロック分割手段602によって、映像フレームと同じ数のブロックに分割された後、入力された暗号鍵により暗号化手段801で暗号化されて、電子透かし埋め込み手段603において、鍵データにより映像フレームに電子透かしとして埋め込まれて出力される。

【0069】図9は、図8の電子透かし埋め込み方式に対応する出力制御方式の第3の実施の形態を示すブロック図である。本方式は、図7の出力制御方式と同様の動作を行うフレーム切り出し手段701、電子透かし抽出手段702、D/A変換手段703、及び図8の暗号化手段801に対応する復号手段901からなる。

【0070】入力された映像データは、フレーム切り出し手段701によりフレームに分割される。電子透かし抽出処理702は、鍵データを用いて各々のフレームより電子透かしとして埋め込まれている音声ブロックを抽出する。抽出された音声ブロックは復号手段901によ

り復号された後、D/A変換手段703により音声信号に変換され、音声出力装置202によって出力される。

【0071】図10は電子透かし埋め込み方式の第5の実施の形態を示すブロック図である。本方式においては、音声ブロックに分割し、ブロック毎に暗号鍵と復号鍵の組を生成し、生成した暗号鍵を用いて音声ブロック再生中に表示されるフレームを暗号化する。また、復号鍵は音声ブロックに電子透かしとして埋め込む。

【0072】本方式は、映像をフレームに分割するフレーム切り出し手段1001、暗号鍵と復号鍵の組を生成する鍵生成手段1002、暗号化手段1003、音声データをブロックに分割するブロック分割手段1004、電子透かし埋め込み手段1005から構成される。ここで用いられる暗号化には、DES等の共通鍵暗号化方式、RSA等の公開鍵暗号化方式が用いられる。

【0073】入力された映像データはフレーム切り出し手段1001によってフレームに、音声データはブロック分割手段1004によってブロックに分割される。一方、鍵生成手段1002では、各々の音声ブロックに対し、暗号鍵と復号鍵の組を生成する。また、暗号化手段1003では、鍵生成手段1002で生成された暗号鍵を用い、音声ブロック再生中に表示される映像フレームを暗号化し出力する。また、電子透かし埋め込み手段1005は、ブロックに分割された音声データへ、鍵生成手段1002で生成された復号鍵を埋め込み出力する。

【0074】図11は、図10の電子透かし埋め込み方式に対応する出力制御方式の第4の実施の形態を示すブロック図である。本方式は、音声データをブロックに分割するブロック分割手段1101、電子透かし抽出手段1102、映像データをフレームに分割するフレーム切り出し手段1103、フレームに施されている暗号を復号する復号手段1104、及び一例としては映像出力装置203によって実行されるD/A変換手段1105から構成される。

【0075】入力された音声データは、ブロック分割手段1101によりブロック毎に分割され、電子透かし抽出手段1102に、透かしの埋め込み位置を示す座標情報等からなる鍵データと共に入力される。電子透かし抽出手段1102では、電子透かしとして埋め込まれている復号鍵を抽出し、復号手段1104に入力する。また、映像データは、フレーム切り出し手段1103によって、フレーム毎に分割された後、復号手段1104に入力され、復号鍵により復号される。復号されたフレームは、D/A変換手段1105によってアナログ信号に変換され、映像出力装置203によって出力される。

【0076】図12は電子透かし埋め込み方式の第6の実施の形態を示すブロック図である。本方式においては、音声ブロックに分割し、ブロック毎に暗号鍵と復号鍵の組を生成し、生成した暗号鍵を用いて音声ブロックを暗号化する。また、復号鍵は音声ブロック再生中に

表示される先頭の映像ブロックに電子透かしとして埋め込む。

【0077】本方式は、音声をブロックに分割するブロック分割手段1201、暗号鍵と復号鍵の組を生成する鍵生成手段1202、暗号化手段1203、映像データから、対応する音声ブロックの先頭にあたるフレームを抽出するフレーム切り出し手段1204、電子透かし埋め込み手段1205、及びフレームの順序を整えるための記憶手段1206から構成される。

【0078】入力された音声データはブロック分割手段1201によってブロック毎に分割される。また、鍵生成手段1202では、音声ブロックと同じ数の暗号鍵と復号鍵の組を生成する。暗号化手段1203では、鍵生成手段1202で生成された暗号鍵を用い、音声ブロックを暗号化し出力する。また、入力された映像データはフレーム切り出し手段1204により音声ブロックの先頭に対応するフレームが抽出され、電子透かし埋め込み手段1205により鍵生成手段1202で生成された復号鍵が埋め込まれ、さらに記憶手段1206に電子透かしが埋め込まれていないフレームと共に入力され、時間的に順序正しく出力される。

【0079】図13は、図12の電子透かし埋め込み方式に対応する出力制御方式の第5の実施の形態を示すブロック図である。本方式は、映像データから音声ブロックの先頭に対応するフレームを抽出するフレーム切り出し手段1301、電子透かし抽出手段1302、音声データをブロックに分割するブロック分割手段1303、音声ブロックに施されている暗号を復号する復号手段1304、及び音声出力装置202によって実行されるD/A変換手段1305から構成される。

【0080】入力された映像データは、フレーム切り出し手段1301により音声ブロックの先頭に対応するフレームが抽出される。抽出されたフレームは、電子透かし抽出手段1302に、透かしの埋め込み位置を示す座標情報等からなる鍵データと共に入力される。電子透かし抽出手段1302では、電子透かしとしてフレームに埋め込まれている復号鍵を抽出し復号手段1304に入力する。

【0081】また、入力された音声データは、ブロック分割手段1303により音声ブロックに分割され、復号手段1304に入力される。音声ブロックは、復号手段1304で、復号鍵により復号され、D/A変換手段1305によりアナログ信号に変換されて、音声出力装置202によって出力される。

【0082】図14は電子透かし埋め込み方式の第7の実施の形態を示すブロック図である。入力された映像データをフレームに分けるフレーム切り出し手段1401、音声データを一定長のブロックに分割するブロック分割手段1402、映像データの指定フレームのハッシュ値を求めるハッシュ計算手段1403、音声ブロック

に映像フレームのハッシュ値を埋め込む電子透かし埋め込み手段1404、電子透かし埋め込み済みの音声ブロックのハッシュ値を求めるハッシュ計算手段1405、映像フレームのあるフレームに音声ブロックのハッシュ値を埋め込む電子透かし埋め込み手段1406、記憶手段1407からなる。

【0083】本方式で用いられているハッシュ値について説明する。ハッシュ値 h とは、ハッシュ関数 $f: x \rightarrow h$ により求められる長い入力列 x の圧縮値である短い出力 h である。また、一方向性関数であり、 $f(x') = f(x)$ を満たす、異なる入力 x, x' を求めるのは難しいという性質を持つ。ハッシュ関数の代表的なものとして、MD5 (Message Digest 5)、SHA (Secure Hash Algorithm) 等がある。ハッシュ関数の詳細については、岡本栄司著「暗号理論入門」(共立出版株式会社)に詳しい。

【0084】入力された映像データは記憶手段1407に保存される他、フレーム切り出し手段1401によって、ハッシュ値を求めるハッシュフレーム及び音声ブロックのハッシュ値が埋め込まれる埋め込みフレームが抽出される。また、音声データはブロック分割手段1402によって、所定長のブロックに分割される。ここで、音声データの1ブロックに対応する時間の中に、ハッシュフレーム、埋め込みフレームが1つずつ存在する様にフレーム抽出、ブロック分割が行われる。

【0085】ハッシュ計算手段1403は、フレーム切り出し手段1401によって求められたハッシュフレームよりハッシュ値を計算する。電子透かし埋め込み手段1404は、電子透かしを埋め込む位置を示す座標情報等からなる鍵データを用いて、ハッシュ値を音声ブロックの中に埋め込む。電子透かしが埋め込まれた音声ブロックは、音声出力として出力される他、ハッシュ計算手段1405に入力されハッシュ値が求められる。求められたハッシュ値は電子透かし埋め込み手段1406に入力され、鍵データによって埋め込みフレームの中に電子透かしとして埋め込まれる。

【0086】電子透かしが埋め込まれた埋め込みフレームは記憶手段1407に記憶されているオリジナルの映像データの対応するフレームと置き換えられて保存される。記憶手段1407に埋め込み対象フレームが保存された後、記憶手段1407に保存されている映像データが映像出力として出力される。

【0087】図15は、図14の電子透かし埋め込み方式に対応する出力制御方式の第6の実施の形態を示すブロック図である。この出力制御方式は、音声データを所定の長さのブロックに分割するブロック分割手段1501、映像データからハッシュフレームと埋め込みフレームを抽出するフレーム切り出し手段1502、音声ブロックのハッシュ値を計算するハッシュ計算手段1503、映像データのハッシュフレームのハッシュ値を計算

するハッシュ計算手段1504、音声ブロックに埋め込まれているハッシュ値を抽出する電子透かし抽出手段1505、埋め込みフレームに埋め込まれている音声ブロックのハッシュ値を抽出する電子透かし抽出手段1506、音声ブロックから計算したハッシュ値と埋め込みフレームから抽出したハッシュ値とを比較する比較手段1507、ハッシュフレームから計算したハッシュ値と音声ブロックから抽出したハッシュ値とを比較する比較手段1508から構成される。

【0088】入力された音声データは、ブロック分割手段1501によって、所定の長さのブロックに分割される。分割されたブロックは1ブロック毎にハッシュ計算手段1503に入力され、ハッシュ値が計算される。同時に電子透かし抽出手段1505にも入力され、電子透かしとして埋め込まれている映像データのハッシュフレームのハッシュ値が抽出される。

【0089】また、入力された映像データはフレーム切り出し手段1502に入力され、ハッシュフレームと埋め込みフレームが抽出される。ハッシュフレームはハッシュ計算手段1504に入力され、ハッシュ値が計算される。また、埋め込みフレームは電子透かし抽出手段1506に入力され、埋め込まれているハッシュ値が抽出される。ハッシュ計算手段1503により計算された音声ブロックのハッシュ値と、電子透かし抽出手段1506により埋め込みフレームより抽出されたハッシュ値は比較手段1507に入力され比較される。

【0090】各ハッシュ値が一致していた場合、即ち、音声データがオリジナルの音声データと一致していると判断される場合は、音声出力装置202が音声を出力するよう制御信号を発する。各ハッシュ値が一致していなかった場合には、音声出力装置202は何も出力せずに、保存していた音声ブロックを捨てるように制御信号を発する。

【0091】また、ハッシュ計算手段1504によりハッシュフレームから計算されたハッシュ値と、電子透かし抽出手段1505により音声ブロックから抽出されたハッシュ値は比較手段1508に入力され比較される。各ハッシュ値が一致していた場合、即ち、映像データがオリジナルの映像データと一致していると判断される場合は、映像出力装置203が映像を出力するよう制御信号を発し、各のハッシュ値が一致していなかった場合は、映像出力装置203は何も出力せずに、保存していたデータを捨てるように制御信号を発する。

【0092】図16は電子透かし埋め込み方式の第8の実施の形態を示すブロック図である。本方式は、図14と同様の動作を行うフレーム切り出し手段1401、ブロック分割手段1402、ハッシュ計算手段1403、電子透かし埋め込み手段1404、ハッシュ計算手段1405、電子透かし埋め込み手段1406、記憶手段1407、及びハッシュ計算手段1403、1405によ

って求めたハッシュ値を暗号化する暗号化手段1601、1602から構成される。

【0093】ハッシュ計算手段1403によって生成されたハッシュフレームのハッシュ値は暗号化手段1601で入力された暗号鍵により暗号化された後、電子透かし埋め込み手段1404によって、音声ブロックに埋め込まれる。また、ハッシュ計算手段1405によって生成された音声ブロックのハッシュ値は暗号化手段1602で入力された暗号鍵により暗号化された後、電子透かし埋め込み手段1406によって埋め込みフレームに埋め込まれる。

【0094】暗号化手段を持ちいたことにより、映像のハッシュフレームを改竄した場合、例えばハッシュ関数が判っても暗号鍵が判らなければ音声ブロックに埋め込むデータを求めることができない。従って、より高度なセキュリティを確保できる。ここで用いられる暗号化には、DES等の共通鍵暗号化方式、RSA等の公開鍵暗号化方式が用いられる。ここで、RSA等の公開鍵暗号方式を用い、その秘密鍵で暗号化を行った場合、求められる値は、デジタル署名となる。

【0095】図17は、図16の電子透かし埋め込み方式に対応する出力制御方式の第7の実施の形態を示すブロック図である。本方式は、図15と同様の動作を行う、ブロック分割手段1501、フレーム切り出し手段1502、ハッシュ計算手段1503、1504、電子透かし抽出手段1505、1506、比較手段1507、1508、及び図16の暗号化手段1601、1602に対応する復号手段1701、1702から成る。

【0096】電子透かし抽出手段1505により音声ブロックから抽出された暗号化されたハッシュフレームは、復号手段1701と入力された復号鍵によって復号される。また、電子透かし抽出手段1506により埋め込みフレームから抽出された、暗号化された音声フレームは復号手段1702と入力された復号鍵によって復号される。以下の動作は図15の出力制御方式と同様である。

【0097】ここで、一例として、電子透かし抽出手段1505、1506によりデジタル署名が抽出された場合、復号手段1701、1702では、署名生成に用いられた秘密鍵に対応する公開鍵で復号を行う。

【0098】図18は、図16の電子透かし埋め込み方式に対応する出力制御方式の第8の実施の形態を示すブロック図である。本方式は、図15と同様の動作を行うブロック分割手段1501、フレーム切り出し手段1502、ハッシュ計算手段1503、1504、電子透かし抽出手段1505、1506、比較手段1507、1508、及び図16と同様の動作を行う暗号化手段1601、1602から構成される。

【0099】ハッシュ計算手段1504により計算されたハッシュ値は、暗号化手段1601に入力され、図1

21

6の電子透かし埋め込み手段で電子透かし埋め込み時に用いた暗号鍵と同一の暗号鍵で暗号化され、比較手段1508に入力される。同様にハッシュ計算手段1503で求められたハッシュ値は、暗号化手段1602で暗号化され、比較手段1507に入力される。他の動作は図15の出力制御方式と同様である。

【0100】ここでは一例として、アナログオーディオビデオコンテンツを扱う電子透かし埋め込み装置及び出力装置を挙げたが、他のアナログコンテンツ、及びデジタルオーディオビデオコンテンツ等デジタルコンテンツ等を扱うデジタルビデオ機器等、その他のコンテンツに対し透かしを埋め込む電子透かし埋め込み装置、制御を行う出力装置等も本発明の範疇に含む。

【0101】また、図1に示した電子透かし埋め込み装置より、A/D変換装置103、104及びD/A変換装置109、110を削除することにより、デジタルコンテンツを扱うデジタル機器に使用可能である電子透かし埋め込み装置が構成される。

【0102】また、図2に示した出力装置より、A/D変換装置204、205を削除することにより、デジタルコンテンツを扱うデジタル出力機器が構成される。また、MPEG-4画像等、複数のオブジェクトを含むコンテンツにおいて、各々のオブジェクトに対し透かしを埋め込み、制御を行う方法及び装置等も本発明の範疇に含む。

【0103】また、図1における埋め込み装置105において、フレーム切り出し手段及びブロック分割手段の代わりに、MPEG-4画像よりオブジェクトを抽出するオブジェクト抽出処理を設けることにより、MPEG-4画像に対する電子透かし埋め込み装置が構成される。また、図2に示した出力装置における出力制御装置がフレーム切り出し手段及びブロック分割手段の代わりにオブジェクトを抽出する処理を行うことにより、MPEG-4画像に埋め込まれた電子透かしにより出力を制御する出力装置が構成される。

【0104】また、上記の電子透かし埋め込み方式を組み合わせることにより、よりセキュリティの高い電子透かし埋め込み方式が構成される。さらに、上記の出力制御方式を組み合わせ用いることにより、上記電子透かし埋め込み方式をこの組み合わせにより生成した電子透かし埋め込み方式によって電子透かしを埋め込んだコンテンツから、電子透かしを抽出し、出力を制御する出力制御方式が容易に構成される。

【0105】次に本発明の他の実施の形態としての記憶媒体について説明する。本発明はハードウェアで構成することもできるが、CPUとメモリとで構成されるコンピュータシステムで構成することもできる。コンピュータシステムで構成する場合、上記メモリは本発明による記憶媒体を構成する。即ち、前述した各実施の形態で説明した動作を実行するためのソフトウェアのプログラム

22

コードを記憶した記憶媒体をシステムや装置で用い、そのシステムや装置のCPUが上記記憶媒体に格納されたプログラムコードを読み出し、実行することにより、本発明の目的を達成することができる。

【0106】また、この記憶媒体としては、ROM、RAM等の半導体メモリ、光ディスク、光磁気ディスク、磁気媒体等を用いてよく、これらをCD-ROM、フロッピーディスク、磁気媒体、磁気カード、不揮発性メモリカード等に構成して用いてよい。

10 【0107】従って、この記憶媒体を各図に示したシステムや装置以外の他のシステムや装置で用い、そのシステムあるいはコンピュータがこの記憶媒体に格納されたプログラムコードを読み出し、実行することによっても、上記各実施の形態と同等の機能を実現できると共に、同等の効果を得ることができ、本発明の目的を達成することができる。

【0108】また、コンピュータ上で稼働しているOS等が処理の一部又は全部を行う場合、あるいは記憶媒体から読み出されたプログラムコードが、コンピュータに挿入された拡張機能ボードやコンピュータに接続された拡張機能ユニットに備わるメモリに書き込まれた後、そのプログラムコードの指示に基づいて、上記拡張機能ボードや拡張機能ユニットに備わるCPU等が処理の一部又は全部を行う場合にも、上記各実施の形態と同等の機能を実現できると共に、同等の効果を得ることができ、本発明の目的を達成することができる。

【0109】

【発明の効果】以上説明したように、本発明によれば、複数の情報系列としての映像及び音声を相互に関連を持たせた電子透かし埋め込みを実現できると共に、映像及び音声を組み合わせた電子透かし埋め込みを実現ことができ、これにより、映像と音声の両方を有するコンテンツの総合的な著作権保護方式が可能となった。

【0110】また、本発明によれば、電子透かしが埋め込まれたコンテンツに改竄等の不正が行われた場合は、それを検知してコンテンツの出力を禁止する等の制御を行うことができる。

【図面の簡単な説明】

40 【図1】本発明による電子透かし埋め込み装置の実施の形態を示すブロック図である。

【図2】本発明による出力制御装置を用いた出力装置の実施の形態を示すブロック図である。

【図3】本発明による電子透かし埋め込み装置で行われる電子透かし埋め込み方式の第1の実施の形態を示すブロック図である。

【図4】本発明による出力制御装置で行われる出力制御方式の第1の実施の形態を示すブロック図である。

50 【図5】電子透かし埋め込み方式の第2の実施の形態を示すブロック図である。

【図6】電子透かし埋め込み方式の第3の実施の形態を示すブロック図である。

【図7】出力制御方式の第2の実施の形態を示すブロック図である。

【図8】電子透かし埋め込み方式の第4の実施の形態を示すブロック図である。

【図9】出力制御方式の第3の実施の形態を示すブロック図である。

【図10】電子透かし埋め込み方式の第5の実施の形態を示すブロック図である。

【図11】出力制御方式の第4の実施の形態を示すブロック図である。

【図12】電子透かし埋め込み方式の第6の実施の形態を示すブロック図である。

【図13】出力制御方式の第5の実施の形態を示すブロック図である。

【図14】電子透かし埋め込み方式の第7の実施の形態を示すブロック図である。

【図15】出力制御方式の第6の実施の形態を示すブロック図である。

【図16】電子透かし埋め込み方式の第8の実施の形態を示すブロック図である。

【図17】出力制御方式の第7の実施の形態を示すブロック図である。

【図18】出力制御方式の第8の実施の形態を示すブロック図である。

【符号の説明】

105 埋め込み装置

108、206 コントローラ

207 出力制御装置

301、401、501、601、701、1001、1103、1204、1301、1401、1502 フレーム切り出し手段

302 フレーム番号生成手段

303、306、505、506、603、1005、1205、1302、1404、1406 電子透かし埋め込み手段

10 埋め込み手段

304、403、502、602、1004、1101、1201、1303、1501 ブロック分割手段

305 ブロック番号生成手段

402、404、702、1102、1302、1505、1506 電子透かし抽出手段

405、1507、1508 比較手段

503 情報入力手段

504 符号化手段

801、1003、1203、1601、1602 暗号化手段

20 符号化手段

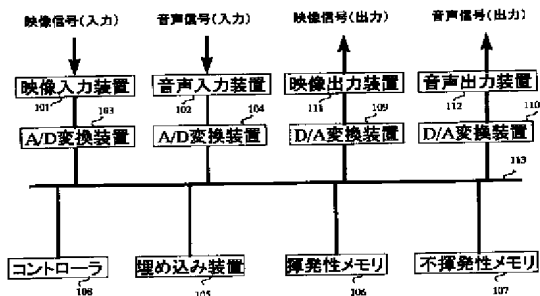
901、1104、1304、1701、1702 復号手段

1002、1202 鍵生成手段

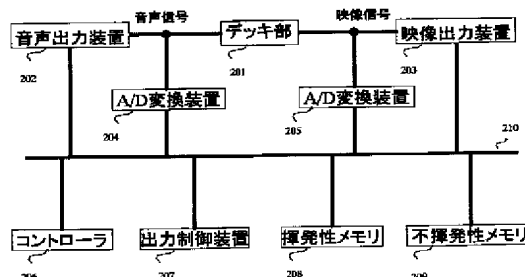
1206、1407 記憶手段

1403、1405、1503、1504 ハッシュ計算手段

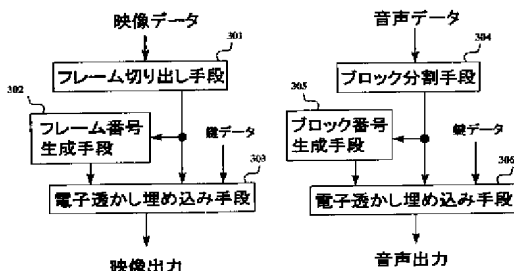
【図1】



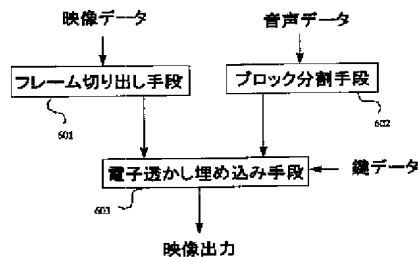
【図2】



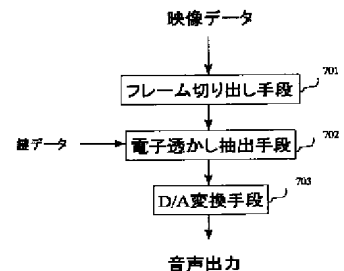
【図3】



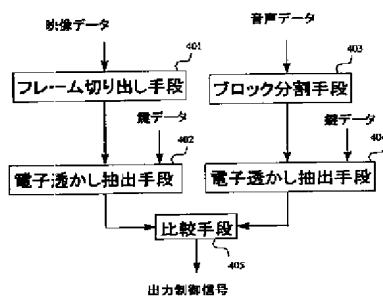
【図6】



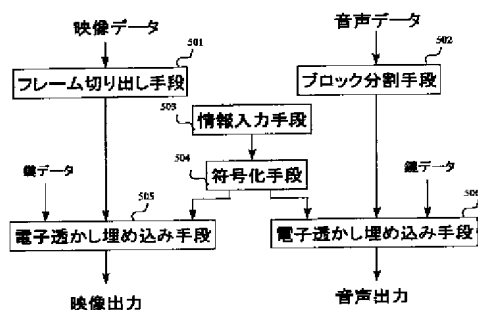
【図7】



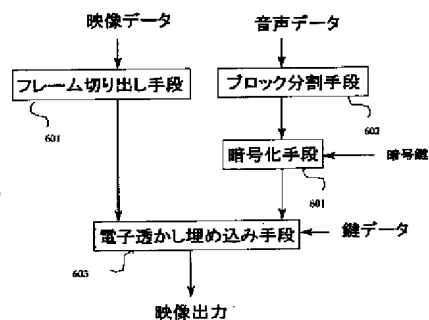
【図4】



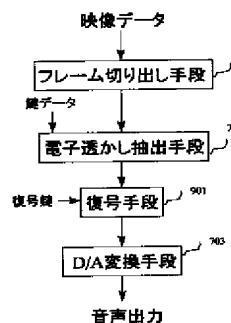
【図5】



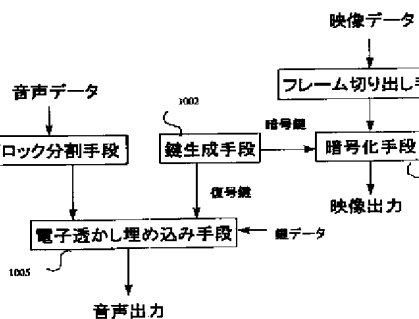
【図8】



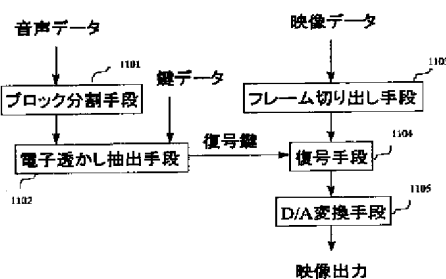
【図9】



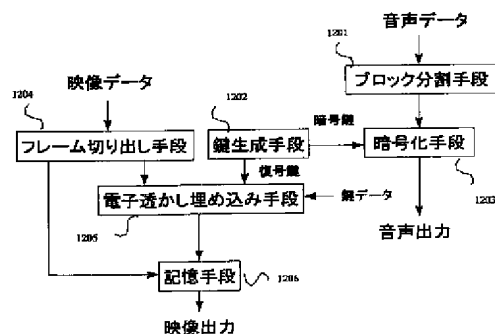
【図10】



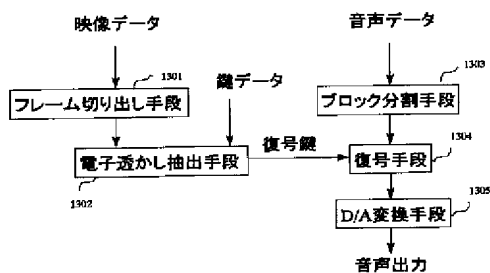
【図11】



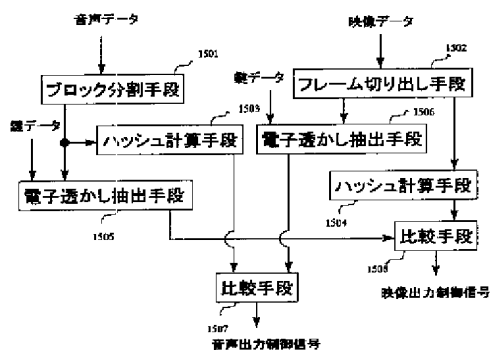
【図12】



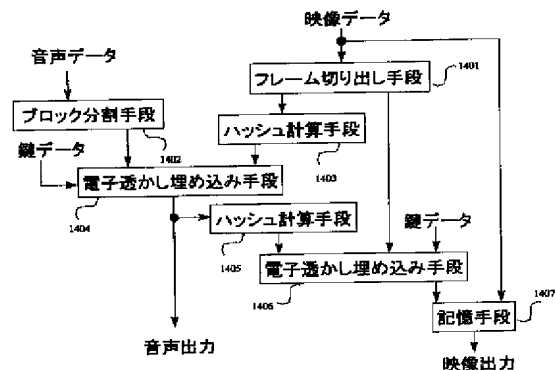
【図13】



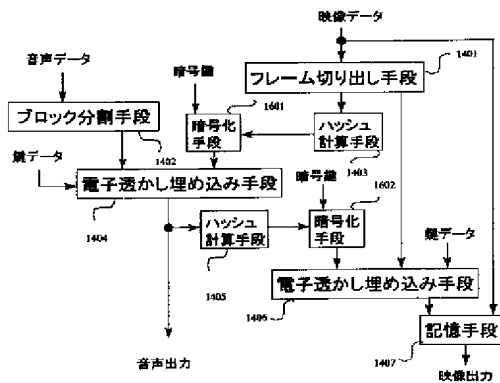
【図15】



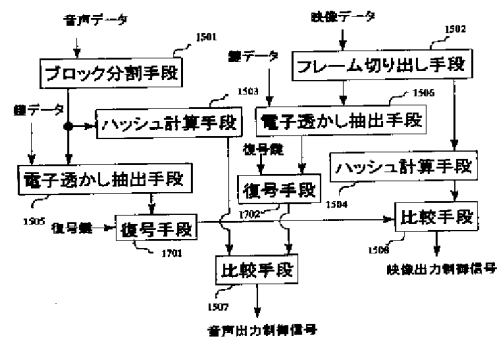
【図14】



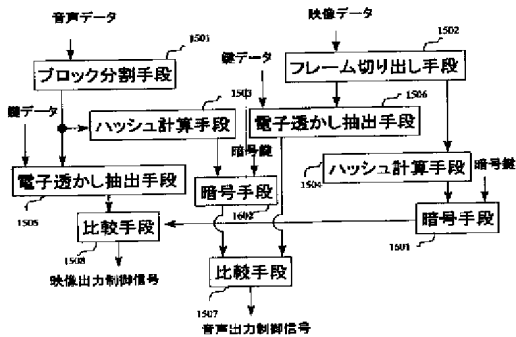
【图 16】



【例 17】



【例 18】



フロントページの続き

F ターム(参考) 5C063 AB03 AB07 AC01 AC05 AC10
CA05 CA09 CA20 CA23 CA40
5C076 AA14 AA40 BA06
5J064 AA00 CA02 CC07
5J104 AA14 EA17 EA20 PA05 PA14
9A001 EE03 EE04 HH15 HH27